بسمه تعالی

مقدمه‌ای بر بدافزارهای RTR – هویت توسعه‌دهنده

بدافزارهای RTR دسته‌ای از بدافزارها هستند که توسط توسعه‌دهنده‌ی متخلفی با نام مستعار RTR منتشر شده‌اند. بر اساس بررسی‌های انجام شده، تاکنون بیش از ۳۰۰ نمونه از بدافزارهای RTR شناسایی شده است. برخی از این بدافزارها در فروشگاه‌های اندرویدی مانند کافه بازار، مایکت، گوگل پلی و ایران اپس منتشر شده‌اند و برخی دیگر از طریق تبلیغات تلگرامی و دانلود خودکار توسط دیگر برنامه‌ها روی دستگاه قربانیان قرار گرفته‌اند. به‌طورکلی بدافزارهای RTR را می‌توان در ۵ شاخه مختلف دسته‌بندی کرد:

۱ بدافزارهای مخفی شونده که از نام‌های مستهجن برای جذب مخاطب استفاده می‌کنند.

۲ نسخه‌های جعلی و غیررسمی تلگرام که از آن‌ها برای فروش عضو، ارسال تبلیغات در گروه‌ها و ... استفاده می‌کنند.

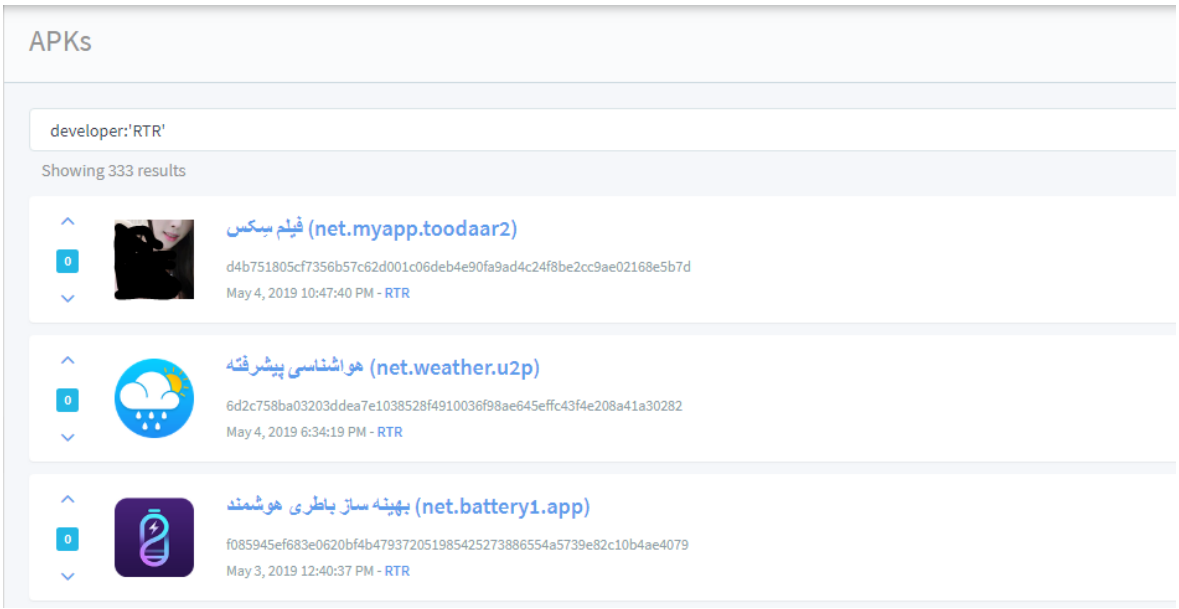
۳ برنامه‌های کاربردی که اغلب با استفاده از سرویس‌های ارسال هشدار، عملیات مخرب مختلفی روی دستگاه قربانی انجام می‌دهند.

۴ بدافزارهای ارزش‌افزوده، که برای چندین شرکت مختلف ارزش‌افزوده، بدافزارهای واسطی را منتشر کرده و از این طریق به عضوگیری برای این سرویس‌ها پرداخته‌اند.

۵ برنامه‌هایی همنام با برنامه‌های محبوب و معروف خارجی مانند برخی پیام‌رسان‌ها.

گزارش مربوط به هر دسته از این بدافزارها متعاقب ارسال خواهد شد. در ادامه به بررسی هویت توسعه دهنده این بدافزارها پرداخته شده است.

با مراجعه به سایت koodous.com متوجه شدیم که توسعه دهنده بسیاری از بدافزارهای شناسایی شده، RTR است. با جستجوی نام این توسعه دهنده، بیش از ۳۰۰ برنامه مخرب شناسایی شدند.



برای دقت بیشتر و حذف شدن مواردی که تشابه اسمی است، گواهی این توسعه دهنده با مقدار sha1 EFEA68B2280EFA2CAB0F130D50E19BE4EEE0B35D جستجو شد.

Certificate

sha1	EFEA68B2280EFA2CAB0F130D50E19BE4EEE0B35D
not_after	Sep 22 13:49:15 2044 GMT
issuerDN	/C=US/L=NEWYORK/O=RTR/CN=RTR
subjectDN	/C=US/L=NEWYORK/O=RTR/CN=RTR
serial	C4210E350898FFA4
not_before	May 8 13:49:15 2017 GMT

نتیجه این جستجو ۱۳۷ برنامه است.

APKs

cert:EFEA68B2280EFA2CAB0F130D50E19BE4EEE0B35D

Showing 137 results

فیلم سکس (net.myapp.toodaar2)
30c3a96291d8516a37edd296ac9806e7533a923fb436f4f276fb30f0e7bd5454
Apr 21, 2019 2:11:07 PM - RTR

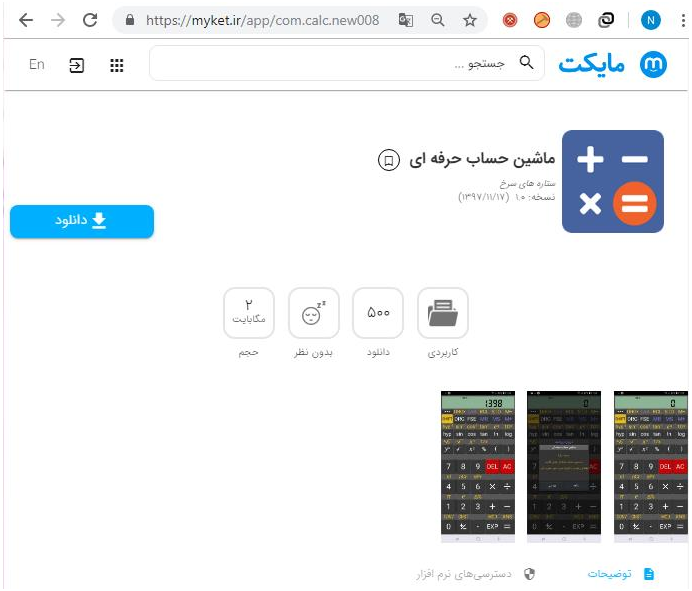
چراغ قوه حرفه ای (com.torch.app_free)
98b70fb1bc39779007717fa3589149d5ce2f92c5abfdedf94701da9cd7d913b8
Apr 19, 2019 2:19:54 PM - RTR

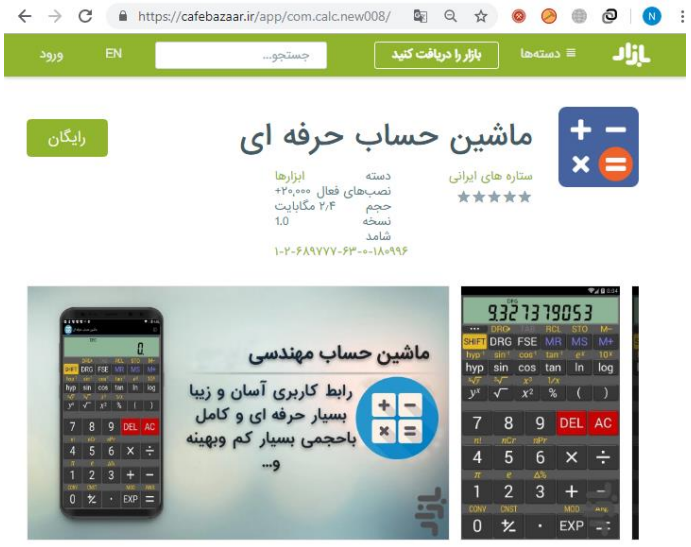
فیلم سکس (net.myapp.toodaar)
776305c7eec1c4e7dc5b8c40d889ad6b6a53f16fe17ddb57daea5c5d4c0536b1
Apr 19, 2019 11:48:16 AM - RTR

تقویم فارسی (com.persiancalendar.topapp)
f8a4548d8ab4cbce49c03dc7945f8109419877b7b3ead6effd13ce66ddd534e1
Apr 19, 2019 11:24:52 AM - RTR

البته این تعداد تنها برنامه‌هایی هستند که با این گواهی منتشر شده‌اند، درحالی که با جستجوی نام بسته‌های برنامه‌ها می‌توان موارد مشابه بیشتری را نیز شناسایی کرد. زیرا در بسیاری از موارد از گواهی‌های عمومی مانند android، Internet Widgits Pty Ltd، Anywhere Software و ... استفاده کرده است.

همان‌طور که گفته شد، برخی از این برنامه‌ها در فروشگاه‌های اندرویدی نیز مشاهده شده‌اند. به عنوان مثال برنامه "ماشین‌حساب حرفه‌ای" با نام بسته com.calc.new008، در فروشگاه کافه بازار (https://cafebazaar.ir/app/com.calc.new008/) و مایکت (https://myket.ir/app/com.calc.new008) منتشر شده است.



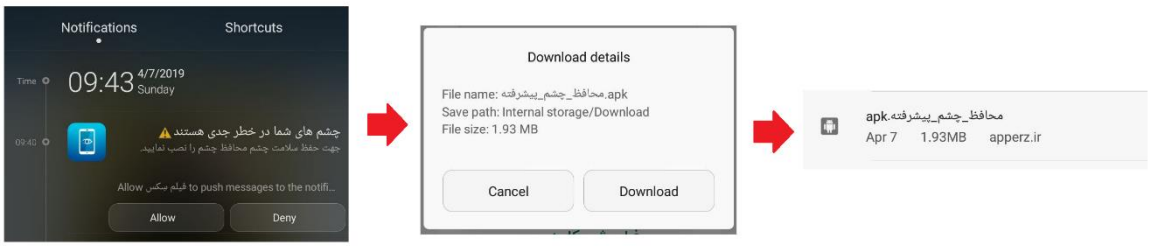


اما اطلاعات شامد این دو برنامه با هم متفاوت است. اطلاعات شامد در مایکت مربوط به علی معتمدی (https://logo.saramad.ir/verify.aspx?CodeShamad=1-2-690695-63-0-15514) و اطلاعات شامد کافه بازار مربوط به نفیسه ابوکاظمی (http://logo.saramad.ir/verify.aspx?CodeShamad=1-2-689777-63-0-180996) است.

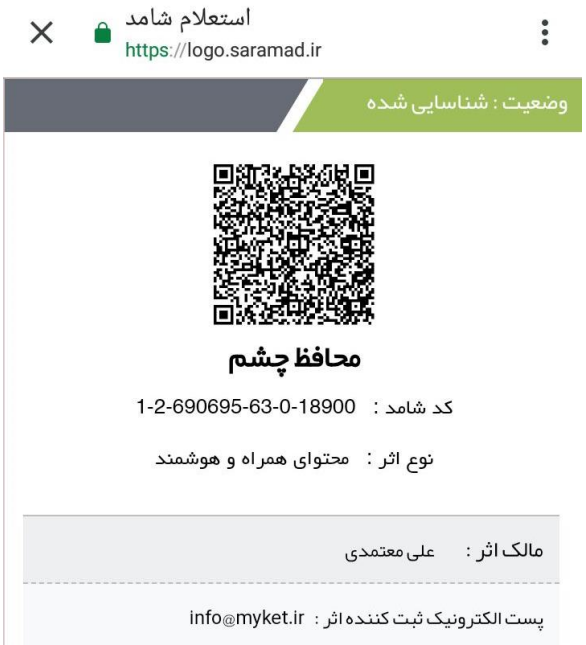
از طرفی ایمیل‌های ثبت شده برای هر دو برنامه vandadproject@gmail.com است. بر اساس همین شواهد به نظر می‌رسد توسعه دهنده ستاره‌های سرخ (https://myket.ir/developer/dev-48244/apps) در مایکت و ستاره‌های ایرانی (https://cafebazaar.ir/developer/091862302639/?l=fa) در کافه بازار متعلق به یک شخص باشند. ایمیل دیگری که در اغلب این برنامه‌ها مشاهده شد، developer1998@yahoo.com است.

علاوه بر این، توسعه دهنده دیگری نیز در بازار با نام زیماگستر (https://cafebazaar.ir/developer/904919034115/?l=fa) وجود دارد که توسعه‌دهنده‌ی برنامه‌های او نیز RTR است. بر اساس اطلاعات شامد (http://logo.saramad.ir/verify.aspx?CodeShamad=1-2-689777-63-0-182230) برنامه‌ها به نام امید حاتم زاده منتشر شده است.

با مشاهده رفتار بدافزارهای این دسته، مشاهده شد که این برنامه‌ها با انتشار هشدارهای مختلف به کاربر، آن‌ها را تشویق به برنامه‌های مختلفی می‌کنند. اغلب این برنامه‌ها از آدرس apperz.ir دانلود می‌شوند.



استعلام شامد این برنامه در مایکت نیز به صورت زیر است:



اطلاعات سایت apperz.ir به شرح زیر است (http://whois.nic.ir/WHOIS?name=apperz.ir):

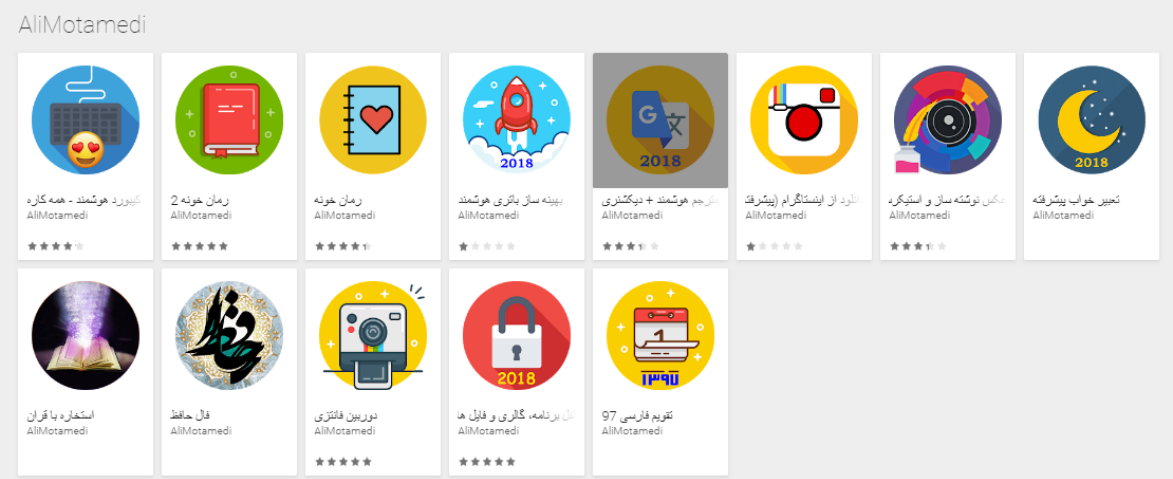
```
domain:         apperz.ir
ascii:          apperz.ir
remarks:        (Domain Holder) ali motamedi
remarks:        (Domain Holder Address) zafar-farid afshar-babak e
sharghi-bonbaste 1-pelak e 1, tehran, tehran, IR

person:         ali motamedi
org:            kheshte honar
e-mail:         aliimotamedi@gmail.com
address:        zafar-farid afshar-babak e sharghi-bonbaste 1-pelak e 1,
tehran, tehran, IR
phone:          09122269602
source:         IRNIC # Filtered
```

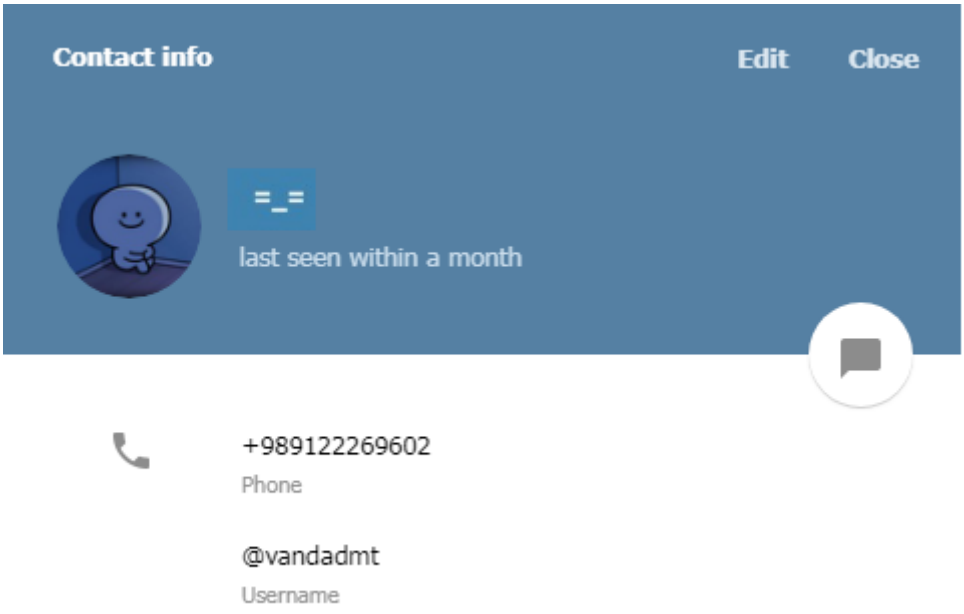
همان‌طور که مشاهده می‌شود، نام علی معتمدی در تمام این موارد مشترک بوده است. آدرس این شخص در اینجا تهران، ظفر، فرید افشار، بابک شرقی، بن‌بست ۱، پلاک ۱ و شماره تلفن ۰۹۱۲۲۲۶۹۶۰۲ ثبت شده است.

علی معتمدی پیش‌ازاین در گوگل پلی نیز برنامه‌هایی منتشر کرده بوده که توسط گوگل حذف شده است (

https://web.archive.org/web/20180712003900/https:/webcache.googleusercontent.com/search?q=cache:lUf9QyBtFwkJ:https://play.google.com/store/apps/developer%3Fid%3DAliMotamedi%26hl%3Duk+&cd=2&hl=en&ct=clnk&gl=gr&lr=lang_en%7Clang_fa&client=firefox-b-ab).

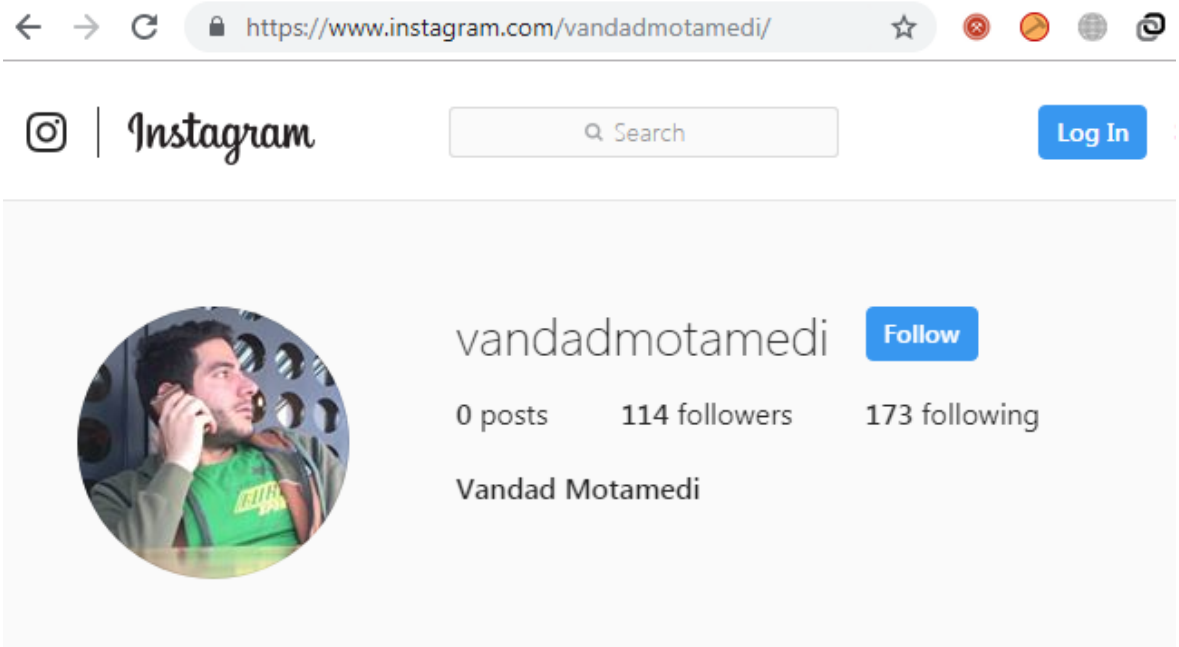


با مشاهده‌ی شماره‌ی ۰۹۱۲۲۲۶۹۶۰۲ در تلگرام حساب کاربری @vandadmt مشاهده می‌شود که با ایمیل vandadproject@gmail.com که در برنامه‌ها وجود داشت، تشابه دارد.



اطلاعات زیر از این حساب کاربری جمع‌آوری شده است:

۱. حساب کاربری اینستاگرام (https://www.instagram.com/vandadmotamedi/)



۲. حساب کاربری لینکدین (https://ir.linkedin.com/in/vandad-motamedi-768613135)

همچنین در اغلب برنامه‌های RTR سعی شده است از طریق سایت‌های baroot.ir و one-signal.ir تحریم‌های مربوط به onesignal.com دور زده شود. ازآنجاکه استفاده از این سایت‌ها تنها در برنامه‌های RTR شایع است و برنامه‌ای با رفتار مشابه مشاهده نشده است، می‌توان این سایت‌ها را نیز به بدافزارهای

RTR مربوط دانست. این دو دامنه روی ip های ۱۶۴.۱۳۲.۱۸۵.۵ و ۱۷۶.۳۱.۸۱.۲ فعال هستند. اطلاعات ثبت دامنه baroot.ir به شرح زیر است:

```
domain:         baroot.ir
ascii:          baroot.ir
remarks:        (Domain Holder) Seyyed Kamal Rezaei
remarks:        (Domain Holder Address) No. 17, 1st Floor, Phase 2, Shahr
Trading Complex, Dariush St.,, Shiraz, Fars, IR
holder-c:       sr209-irnic
admin-c:        sr209-irnic
tech-c:         sa1601-irnic
bill-c:         sa1601-irnic
nserver:        alex.ns.cloudflare.com
nserver:        linda.ns.cloudflare.com
last-updated:   2019-03-24
expire-date:    2020-04-18
source:         IRNIC # Filtered
e-mail:         skrsoft20@gmail.com
phone:          09390600441
```

اطلاعات سایت one-signal.ir نیز به صورت زیر است:

```
domain:         one-signal.ir
ascii:          one-signal.ir
remarks:        (Domain Holder) Seyyed Kamal Rezaei
remarks:        (Domain Holder Address) No. 17, 1st Floor, Phase 2, Shahr
Trading Complex, Dariush St.,, Shiraz, Fars, IR
holder-c:       sr209-irnic
admin-c:        sr209-irnic
tech-c:         sa1601-irnic
bill-c:         sa1601-irnic
nserver:        alex.ns.cloudflare.com
nserver:        linda.ns.cloudflare.com
last-updated:   2019-03-03
expire-date:    2019-08-20
source:         IRNIC # Filtered
e-mail:         skrsoft20@gmail.com
phone:          09390600441
```

از آنجایی که بدافزارهای ارزش‌افزوده‌ای با نام توسعه دهنده RTR شناسایی شده است، احتمال می‌رود علی معتمدی یا ونداد معتمدی در شرکت تبلیغاتی‌ای فعال باشد که توانسته است با شرکت‌های ارزش‌افزوده‌ی مختلف قرارداد بسته و برای آن‌ها عضوگیری کند. اما متاسفانه تاکنون اطلاعاتی راجع به این شرکت احتمالی پیدا نشده است.